

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

11000 U.S. PTO
09/864304
05/25/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

2000年 5月29日

出願番号
Application Number:

特願2000-158770

出願人
Applicant(s):

株式会社日立製作所

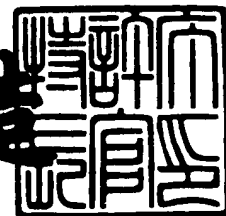
U.S. Appln Filed 5-25-01
Inventor: T. Oishi et al
Mattingly Stanger & Malor
Docket ASA-1004

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 4月13日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3029530

【書類名】 特許願
 【整理番号】 H00010271
 【あて先】 特許庁長官殿
 【国際特許分類】 G03F 3/00
 H04L 12/00

【発明者】
 【住所又は居所】 東京都小平市上水本町5丁目22番1号 株式会社 日立超エル・エス・アイ・システムズ内
 【氏名】 大石 敏久

【発明者】
 【住所又は居所】 東京都青梅市新町六丁目16番地の3 株式会社日立製作所 デバイス開発センタ内
 【氏名】 戸澤 淳

【発明者】
 【住所又は居所】 東京都青梅市新町六丁目16番地の3 株式会社日立製作所 デバイス開発センタ内
 【氏名】 柴山 哲也

【発明者】
 【住所又は居所】 東京都小平市上水本町5丁目22番1号 株式会社 日立超エル・エス・アイ・システムズ内
 【氏名】 濱田 真人

【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社 日立製作所

【代理人】
 【識別番号】 100085811
 【弁理士】
 【氏名又は名称】 大日方 富雄
 【電話番号】 03-3269-1430

【手数料の表示】

【予納台帳番号】 027177

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証通信用半導体装置

【特許請求の範囲】

【請求項 1】 1 個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するとともに外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および復合化を行なう暗号処理部と、所定のプロトコルに従って上位層または下位層との通信を行なうインタフェース部とが形成されていることを特徴とする認証通信用半導体装置。

【請求項 2】 1 個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するとともに外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および復合化を行なう暗号処理部と、所定のプロトコルに従って上位層との通信を行なう第 1 のインタフェース部と、所定のプロトコルに従って下位層との通信を行なう第 2 のインタフェース部とが形成されていることを特徴とする認証通信用半導体装置。

【請求項 3】 上記主処理部は、鍵生成アルゴリズムおよびデータ送受信を要求する外部装置の認証を行なう認証アルゴリズムを具現化するプログラムを格納した不揮発性メモリと、上記プログラムに従って鍵コードを生成および外部装置とのデータの送受信の認可／非認可の決定を行なうプログラム実行型の制御手段と、該制御手段の作業領域を提供する揮発性メモリとから構成され、

上記不揮発性メモリ、上記制御手段、上記揮発性メモリ、上記暗号処理部および上記インタフェース部は内部バスを介して互いに接続されていることを特徴とする請求項 1 または 2 に記載の認証通信用半導体装置。

【請求項 4】 上記暗号処理部は、上記主処理部で生成された鍵コードが設定されるレジスタを備え、該レジスタに上記バスを介して設定された鍵コードに基づいて送受信データの暗号化および復合化を行なうように構成されていることを特徴とする請求項 3 に記載の認証通信用半導体装置。

【請求項 5】 上記インタフェース部は、通信制御コードが設定されるレジ

スタを備え、該レジスタに上記主処理部によって上記バスを介して設定された通信制御に基づいて通信を行なうように構成されていることを特徴とする請求項 3 または 4 に記載の認証通信用半導体装置。

【請求項 6】 上記内部バスが結合された外部端子を備えていることを特徴とする請求項 5 に記載の認証通信用半導体装置。

【請求項 7】 請求項 6 に記載の認証通信用半導体装置と、上記内部バスが結合された外部端子に接続された外部メモリとを備え、該外部メモリには通信路の設定を含む通信制御プログラムが格納され、該プログラムに従って上記主処理部が上記インタフェース部の上記レジスタに通信制御コードを設定することにより外部装置との通信が行なわれるように構成されていることを特徴とする電子機器。

【請求項 8】 単一の半導体チップに形成され、暗号鍵コードによって暗号時は平文データを暗文データに暗合化し、復号時は暗文データを平文データに復号化し、暗号化および復号化の必要がない場合はデータをそのまま素通りさせる暗号処理部を備え、前記暗号処理部の暗文データには、通信の下位層とプロトコルを司る下位層インターフェース部が接続され、前記暗号処理部の平文データには、通信の上位層とプロトコルを司る上位層インターフェース部が接続され、前記下位層インターフェース部は、前記半導体チップの外部の通信信号を制御する下位層デバイスとの間で暗文データの伝送を行う下位層通信路を少なくともひとつ備え、前記上位層インターフェース部は、前記半導体チップの外部の上位層デバイスと平文データの伝送を行う上位層通信路を少なくともひとつ備え、下位層を経由する通信の認証処理および前記暗号処理部の鍵生成処理を行う鍵生成処理部を備え、前記鍵生成処理部は CPU、ROM、RAM で構成され、前記 CPU は、前記暗号処理部が暗号鍵を保持する鍵レジスタの設定と、前記下位層インターフェース部および上位層インターフェース部が備える制御レジスタの設定を、前記 CPU、前記暗号処理部、前記下位層インターフェース部および前記上位層インターフェース部とを接続するバスを経由して行なうように構成されていることを特徴とした認証通信用半導体装置。

【請求項 9】 前記単一の半導体チップに形成され、前記半導体チップの前

記上位層インターフェース部に、更に暗号処理部を経由せず前記下位層インターフェース部から前記上位層インターフェース部に第 1 の上位層ー下位層通信路と第 2 の上位層ー下位層通信路が接続され、前記上位層インターフェース部は、前記半導体チップの外部の上位層デバイスとの間の信号伝送を行う第 1 の上位層通信路と第 2 の上位層通信路を備え、第 1 の上位層通信路は暗号処理部からのデータかあるいは暗号処理部を経由しない下位層インターフェースからのデータかを選択でき、第 2 の上位層通信路は前記第 1 の上位層ー下位層通信路からのデータかあるいは前記第 2 の上位層ー下位層通信路からのデータかを選択できることを特徴とする請求項 8 の認証通信用半導体装置。

【請求項 1 0】 前記単一の半導体チップに形成され、前記暗号処理部に第 1 の暗号処理回路と第 2 の暗号処理回路を備え、前記上位層インターフェース部に第 1 の上位層インターフェース回路と第 2 の上位層インターフェース回路を備え、前記第 1 の暗号処理回路の平文データの通信路を前記第 1 の上位層インターフェース回路に接続し、前記第 2 の暗号処理回路の平文データの通信路を前記第 2 の上位層インターフェース回路に接続し、前記第 1 の上位層インターフェース部に前記半導体チップの外部の第 1 の上位層デバイスとの間の信号伝送を行う第 1 の上位層通信路と、前記第 2 の上位層インターフェース部に前記半導体チップの外部の第 2 の上位層デバイスとの間の信号伝送を行う第 2 の上位層通信路とを備えることを特徴とする請求項 8 の認証通信用半導体装置。

【請求項 1 1】 前記バスに接続されて電氣的に書換え可能な不揮発メモリが同一半導体チップ上に形成されていることを特徴とする請求項 8 の認証通信用半導体装置。

【請求項 1 2】 前記下位層デバイスを同一半導体チップ上に備え、前記下位層デバイスからの間の信号伝送を行う通信路を少なくともひとつ備えることを特徴とする請求項 8 の認証通信用半導体装置。

【請求項 1 3】 請求項 8 ～ 1 2 のいずれかに記載の認証通信用半導体装置と、前記下位層デバイスと、該下位層デバイスと結合され外部から通信用伝送媒体が接続可能なコネクタとを備えたことを特徴とする電子機器。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、データ処理技術さらには暗号鍵コードを用いたデジタルデータの暗号化／復号化処理に適用して有効な技術に関し、例えば I E E E 1 3 9 4 (Institute of Electrical and Electronics Engineers 1394)規格のシリアルバスを介して接続される電子機器の間で通信の安全性を保証しつつ送受信するための通信用半導体装置およびそれを用いたシステムに利用して有効な技術に関する。

【 0 0 0 2 】

【従来の技術】

I E E E 1 3 9 4 規格は、音声や映像などのデジタルデータを、ケーブルを介して A V 機器などの電子機器間でシリアル伝送するための規格である。近年、I R D (Integrated Receiver Decoder)や D - V H S (Digital-VHS)、D V (Digital Video)カムコーダーなどの電子機器を I E E E 1 3 9 4 規格のシリアルバスを介して接続し、デジタル音声データやデジタル映像データなどのデジタルコンテンツを、例えば I S O / I E C (International Standardization Organization/ International Electrotechnical Commission)13818規格の MPEG2-TS (Moving Picture Experts Group 2 Transport Stream)や IEC61883規格に準拠したパケットなどに乗せて送受信を行うことができるようにした電子機器が提案されている。

【 0 0 0 3 】

ところで、映画などの著作物を記憶するデジタルビデオテープやディスク等のメディアおよびその再生装置においては、著作権の保護の見地から違法なコピーを防止するための技術が不可欠である。近年、デジタルコンテンツの著作権保護のため、不正コピー防止技術が、例えば家電業界、パソコン業界および映画業界などが組織する業界団体である C P T W G (Copy Protection Technical Working Group)などで標準化が進められている。C P T W G が中心となって決めた不正コピー防止技術では、DVD-Videoの C S S (Content Scrambling System)仕様や I E E E 1 3 9 4 向けの 5 C - D T C P (5 Company Digital Transmission Copy Protection)仕様が、現在実用化されている。

【 0 0 0 4 】

しかしながら、DVD-Videoの不正コピー防止技術であるCSSに関しては、クラッカー（悪意をもって不正アクセスなどを行うハッカーのこと）などによりCSSのセキュリティを破るソフトウェアが作られ、米国やフランスなどで、インターネット上の複数のWWWサーバで配布され産業界に深刻な打撃を与えている（日経BP社発行、日経エレクトロニクス、1999.11.1、No756、第23頁参照）。そのため、CSSや5C-DTPCのようにセキュリティ技術が標準化され全く同じ技術を使用したAV機器が大量に出回る場合は、クラッカーの不正コピー防止攻撃に対する安全性の高さが、デジタルコンテンツの著作権保護の観点からAV機器に対し求められている（日経BP社発行、日経エレクトロニクス、2000.3.27、No766、P152～P163参照）。

【 0 0 0 5 】

また、著作物不正コピーの悪質な例では、CD (Compact Disc) に収められたゲームソフトの不正コピーを可能とするためのハード的な改造を某社製のゲーム機器に施したものが不正に売買されており、ゲームソフトの著作権保護が破られている。このように、近年においては、ソフトウェアによる不正コピーのみならず、電子機器のハードウェアの改造による手段に及んでまで不正コピー防止技術に対する攻撃の可能性がある（技術評論社発行、「暗号のすべてがわかる本」、初版第1刷、第126～128頁参照）。

【 0 0 0 6 】

一方、5C-DTPCに関しては、以下のようなシステムが実用化されている。図13に、従来の5C-DTPC仕様の認証通信装置とそれを用いたシステムとしてのAV機器の概略構成を示す。図13において、符号72で示されているのは5C-DTPC仕様の通信用半導体装置（通信装置）、71は認証処理を行なうマイクロコンピュータチップからなる認証装置である。該認証装置71と上記通信装置72は、デジタルビデオテープレコーダやセットトップボックスなどのAV機器に搭載される。

【 0 0 0 7 】

通信装置72は、図13に示されているように、IEEE 1394 シリアルバス731との接続を行なう下位層インタフェース回路100と、外部デバイスと

の接続を行なう上位層インタフェース回路 2 0 0 と、暗号処理回路 3 0 0 とからなり、I E E E 1 3 9 4 規格のケーブル 7 3 0 が接続されるポート 7 1 1 ~ 7 1 3 を有する物理層としての 1 3 9 4 P H Y チップ 7 0 0 と M P E G 2 デコーダやコーデック、D V コーデックなどを有するディスプレイ装置のような外部デバイス 9 0 との間に接続されて、I E E E 1 3 9 4 ケーブル 7 3 0 から送られてくる暗号化されたデジタルデータを復号化して外部デバイス 9 0 へ伝える機能を有する。下位層インタフェース回路 1 0 0 と上位層インタフェース回路 2 0 0 と暗号処理回路 3 0 0 は別のチップで構成されることもある。認証装置 7 1 は、通信装置 7 2 と外部バス 4 1 を介して接続され、暗号処理回路 3 0 0 で必要とされる暗号鍵コード（以下、単に暗号鍵と称する）を生成したりデータを受信したい A V 機器からの要求に応じて認証処理を行なう機能を有する。

【 0 0 0 8 】

【発明が解決しようとする課題】

しかしながら、上記従来の 5 C - D T P C 仕様のシステム（認証通信装置）にあっては、通信装置 7 2 が認証装置 7 1 とは別のチップで構成されており、バス 4 1 を介して認証装置 7 1 や R A M 7 5 0、電氣的に書換え可能なフラッシュ R O M 7 4 0 と接続されていた。そして、通信装置 7 2 内のインタフェース回路 1 0 0 と 2 0 0 にはそれぞれ制御用レジスタ 1 4, 2 4 が、また暗号処理回路 3 0 0 には鍵レジスタが 3 4 設けられており、これらのレジスタにバス 4 1 を介して制御データや暗号化／復号化用の暗号鍵コードが認証装置 7 1 によって設定されることで、暗号化、復号化処理などの動作を行なうように構成されていた。

【 0 0 0 9 】

そのため、上記従来の 5 C - D T P C 仕様の認証通信装置は、暗号処理回路 3 0 0 とバス 4 1 とが接続される外部端子 6 2 の信号を監視することで、秘匿性を有する暗号鍵が知られてしまったり暗号処理のアルゴリズムが解析されてしまうおそれがある。具体的には、図 1 0 の A V 機器の構成において、ロジック・アナライザなどの計測機器を用いて、通信装置 7 2 の外部端子 6 2 の信号や C P U バス 4 1 のバス上のデータがモニタされるなどして、認証動作過程での通信コマンド、暗号交換鍵および乱数値などが窃取されることにより認証装置のセキュリティ

ィへの攻撃の手掛かりを得るための解析ができる余地を許している。

【 0 0 1 0 】

前記攻撃により認証動作を不正に回避する不正装置が作成された場合、例えば、図 1 4 のように A V 機器 8 0 0 A および 8 0 0 B に、それぞれ C P U バス 4 1 と認証装置 7 1 に接続された不正装置 7 5 を設けるとともに、各 C P U バス 4 1 - 4 1 間にジャンパー線 4 6 等の不正な接続線を設けるなどの改造がなされ、認証動作過程の通信コマンドが不正装置 7 5 からそれぞれの認証装置 7 1 へ発行されることで正規の認証が回避され、認証を不正に成立させる。その後、デジタルコンテンツが暗号処理回路 3 0 0 で暗号化および復号化される段階では、各不正装置 7 5 が認証装置 7 1 へ、C P U バス 4 1 のバス権を譲るように要求するバス権要求信号の発行を行なって、認証装置 7 1 から C P U バス 4 1 のバス権を奪った後、正常の認証成立後に使用される暗号鍵の代わりとして、不正装置 7 5 間で共有する不正鍵を使用することで、デジタルコンテンツが A V 機器 8 0 0 A から 8 0 0 B へ不正に送信されるおそれがあるという課題があることが明らかとなった。

【 0 0 1 1 】

本発明の 1 つの目的は、外部端子を監視していても暗号鍵や制御データを読み取ることができないようにして、悪質なアクセスを行うクラッカーによるデジタルコンテンツの著作権保護のための不正コピー防止技術に対する攻撃手掛かりとなる解析を抑止してデジタルコンテンツの不正なコピーを防止可能な認証通信装置を提供することにある。

【 0 0 1 2 】

また、本発明の他の目的は、ハードウェアの改造により不正コピー防止技術が破られることを抑止するための認証通信装置を提供することにある。

【 0 0 1 3 】

この発明の前記ならびにそのほかの目的と新規な特徴については、本明細書の記述および添附図面から明らかになるであろう。

【 0 0 1 4 】

【課題を解決するための手段】

本願において開示される発明のうち代表的なものの概要を説明すれば、下記の
とおりである。

【 0 0 1 5 】

すなわち、上記課題を解決するために、本発明の認証通信用半導体装置は、1
個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するととも
に外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主
処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および
復合化を行なう暗号処理部と、所定のプロトコルに従って上位層または下位層と
の通信を行なうインターフェース部とを形成したものである。

【 0 0 1 6 】

より具体的には、単一の半導体チップに形成され、暗号鍵コードによって暗号
時は平文データを暗文データに暗合化し、復号時は暗文データを平文データに復
号化し、暗号化および復号化の必要がない場合はデータをそのまま素通りさせる
暗号処理部を備え、前記暗号処理部の暗文データには、通信の下位層とプロトコ
ルを司る下位層インターフェース部が接続され、前記暗号処理部の平文データに
は、通信の上位層とプロトコルを司る上位層インターフェース部が接続され、前
記下位層インターフェース部は、前記半導体チップの外部の通信信号を制御する
下位層デバイスとの間で暗文データの伝送を行う下位層通信路を少なくともひとつ
備え、前記上位層インターフェース部は、前記半導体チップの外部の上位層デ
バイスと平文データの伝送を行う上位層通信路を少なくともひとつ備え、下位層
を経由する通信の認証処理および前記暗号処理部の鍵生成処理を行う鍵生成処理
部を備え、前記鍵生成処理部はCPU、ROM、RAMで構成され、前記CPU
は、前記暗号処理部が暗号鍵を保持する鍵レジスタの設定と、前記下位層インタ
ーフェース部および上位層インターフェース部が備える制御レジスタの設定を、
前記CPU、前記暗号処理部、前記下位層インターフェース部および前記上位層
インターフェース部とを接続するバスを経由して行なうように構成したものであ
る。

【 0 0 1 7 】

上記した手段によれば、半導体チップの内部信号を外部から窃取しにくいとと

もに、認証処理過程の通信コマンドや暗号処理過程の暗号鍵設定を認証通信用 L S I の外部から改竄して入力することが困難であるので、不正コピー防止技術を破るために認証処理過程を解析することが困難となり、また、電子機器を改造して不正コピー防止技術を破ることが難しくなり、これによって、著作権保護を必要とするデジタルコンテンツを高い安全性の下に送受信できる電子機器を実現することができる。

【 0 0 1 8 】

また、当該半導体装置が搭載される電子機器の固有情報等を記憶するための電氣的に書き換え可能な不揮発性メモリを必要とする場合に、その不揮発性メモリも同一チップ上に形成する。これにより、当該電子機器の固有情報を、外部から窃取されるのを防止することができる。また、電氣的に書き換え可能な不揮発性メモリであるため、機器毎に異なる固有情報を書き込むことでセキュリティを向上させることが容易であり、かつ低コストで済む。この不揮発性メモリは、予め固有情報を書込んだ状態で機器に組み込むようにすることができる。

【 0 0 1 9 】

さらに、鍵コードの生成や外部装置の認証並びに通信制御を行なう上記主処理部と上記暗号処理部および上記インタフェース部とが内部バスを介して互いに接続されており、当該半導体装置が搭載される電子機器の固有情報等を記憶するための電氣的に書き換え可能な不揮発性メモリを必要とする場合に、その不揮発性メモリが接続される外部端子と上記内部バスとの間にバスの切換えを制御するバス制御回路を設ける。これにより、暗号処理過程や認証処理過程が外部から窃取されるのを防止できるとともに、暗号処理過程での暗号鍵や認証処理過程の通信制御コードをチップの外部から改竄して入力することが困難となり、クラッカーによる暗号処理や認証処理の解析および装置の改造といった攻撃を抑止することが可能となり、著作権保護を必要とするデジタルコンテンツの不正コピーに対する安全性が高まる。

【 0 0 2 0 】

さらに、当該半導体装置が搭載される電子機器のシステム全体を制御するホスト CPU が別途必要であり、当該半導体装置の上記主処理部が、鍵生成アルゴリ

ズムおよびデータ送受信を要求する外部装置の認証を行なう認証アルゴリズムを具現化するプログラムを格納した不揮発性メモリと、上記プログラムに従って鍵コードを生成および外部装置とのデータの送受信の認可／非認可の決定を行なうプログラム実行型の制御手段と、該制御手段の作業領域を提供する揮発性メモリとから構成されているような場合に、上記制御手段とホストCPUとの間の通信を行なう通信回路をホストCPUとの通信ポートと上記内部バスとの間に設ける。これによって、ホストCPUとの通信ポートを有する半導体装置において、当該通信ポートから暗号処理過程や認証処理過程が外部から窃取されるのを防止することができるとともに、暗号処理過程での暗号鍵や認証処理過程の通信制御コードをチップの外部から改竄して入力することが困難となり、クラッカーによる暗号処理や認証処理の解析および装置の改造といった攻撃を抑止することが可能となる。

【0021】

しかもこの場合、上記制御手段は、限られた所定のコマンド以外を受付けないように構成する。これにより、暗号処理過程や認証処理過程でチップ外部から不正な介入を行なうことが困難となり、安全性が向上する。

【0022】

【発明の実施の形態】

以下、本発明の好適な実施例を図面に基づいて説明する。

【0023】

図1は、本発明を適用した5C-DTPC仕様の認証通信用LSI（大規模半導体集積回路）の第1の実施形態を示す。

【0024】

本実施例においては、中央処理ユニットCPU500および作業領域を提供するRAM502、プログラムや固定データを格納するROM501からなり暗号鍵を生成したり外部の装置との間のデータの送受信の認可／非認可を決定するための認証処理や通信制御などの機能を有する鍵生成&認証処理部50と、IEEE1394シリアルバスとの接続を行なう下位層インタフェース部10と、外部デバイスとの接続を行なう上位層インタフェース部20と、暗号鍵を用いてデー

タの暗号化および複合化処理を行なう暗号処理部 3 0 と、これらの回路間を接続する内部バス 4 1 とが、単結晶シリコンのような 1 個の半導体チップ上に形成され、認証通信用 L S I を構成している。

【 0 0 2 5 】

さらに、通信路の設定などの通信制御プログラムや機器に関する固有情報等を記憶するための電氣的に書換え可能なフラッシュメモリのような不揮発性の外部メモリ 7 4 0 が上記内部バス 4 1 と接続されているとともに、上記下位層インタフェース部 1 0 には I E E E 1 3 9 4 規格のケーブル 7 3 0 が接続されるポート 7 1 1 ~ 7 1 3 を有する物理層としての 1 3 9 4 P H Y (I E E E 1 3 9 4 P h y s i c a l L a y e r P r o t o c o l) チップ 7 0 0 が、また上位層インタフェース部 2 0 には M P E G 2 デコーダやコーデック、D V コーデックなどの外部デバイス 9 0 を記録再生装置 4 0 が接続されて、A V 機器が構成される。

【 0 0 2 6 】

下位層インターフェース部 1 0 は、パケット形態でデータの送受信を行なえるようにデータを処理するパケット処理回路 1 0 1 と、下位層バス 1 2 を介して 1 3 9 4 P H Y チップ 7 0 0 と接続され I E E E 1 3 9 4 ケーブルとの接続のための制御を行なうリンク層としての 1 3 9 4 リンク回路 1 0 0 と、で構成される。1 3 9 4 P H Y チップ 7 0 0 は、データのマルチプレックスやデマルチプレックスなど物理層としての制御を行なう半導体チップで、特に制限されるものでないが、本実施例では 3 つの I E E E 1 3 9 4 仕様のポート 7 1 1, 7 1 2 および 7 1 3 を備えている。これらのポートと I E E E 1 3 9 4 仕様のケーブル（以下、1 3 9 4 ケーブルと称する）との具体的な接続の仕方は、図 1 3 の従来例と同様である。すなわち、各ポート 7 1 1, 7 1 2 および 7 1 3 は、それぞれ I E E E 1 3 9 4 仕様のソケット 7 2 1, 7 2 2 および 7 2 3 からなるコネクタ部 7 2 0 に接続されている。

【 0 0 2 7 】

ユーザは、I E E E 1 3 9 4 コネクタ部 7 2 0 の空きソケットの何れか、例えばソケット 7 2 1 に 1 3 9 4 ケーブル 7 4 1 の一端である 1 3 9 4 プラグ 7 3 1 を接続し、非接続側の一端である 1 3 9 4 プラグ 7 5 1 を他の A V 機器の I E E

E 1 3 9 4 コネクタ部に接続することで、図 7 に示すように A V 機器 8 0 0 A と 8 0 0 B との間でデジタルコンテンツおよび通信コマンドを送受信するための伝送路としての 1 3 9 4 バス 8 1 0 を確保できる。また、1 3 9 4 ケーブル 7 4 1 のプラグ 7 3 1 をこのソケット 7 2 1 から引き抜くことで、当該 A V 機器を 1 3 9 4 バスから解放することができる。なお、図 7 の A V 機器間の 1 3 9 4 バスの接続図では、説明を簡単にするため 2 つの A V 機器で説明を進めるが、本発明は下位層の通信プロトコルで規定されるバスのトポロジーが 2 つに限定されるものでなく、1 3 9 4 バス 8 1 0 上には、他の電子機器が同様にして接続される。

【 0 0 2 8 】

上位層インターフェース回路 2 0 0 は、1 3 9 4 P H Y チップ 7 0 0 の物理層や 1 3 9 4 リンク回路 1 0 0 のリンク層より上位の層へデジタルコンテンツを渡すためのインターフェース回路で、上位層バス 2 2 を介して M P E G 2 C O D E C (CODER DECODER) や D V C O D E C などの外部デバイス 9 0 と接続され、外部デバイス 9 0 は記録再生装置 4 0 0 へ接続される。記録再生装置 4 0 0 では、映像や音声のデジタルコンテンツを記録または再生する。

【 0 0 2 9 】

上記インタフェース部 1 0 と 2 0 にはそれぞれ制御用レジスタ 1 4 , 2 4 が設けられており、鍵生成&認証処理部 5 0 の C P U 5 0 0 が内部バス 4 1 を介して制御レジスタ 2 4 および 1 4 に制御コードを設定することで、1 3 9 4 リンク回路 1 0 0 および上位層インターフェース回路 2 0 0 の通信路の設定を行う。下位層の通信制御プログラムは外部メモリ 7 4 0 に格納されており、C P U 5 0 0 は、外部メモリ 7 4 0 内の下位層の通信制御プログラムに従って制御レジスタ 1 4 を設定し、下位層デバイスを経由して 1 3 9 4 バス 8 1 0 上の電子機器との通信を行う。具体的には、1 3 9 4 バス上の電子機器へ通信コマンドを発行し、例えばその電子機器の録画、再生、電源のオン/オフなどを制御したりその電子機器の情報を閲覧したりする。

【 0 0 3 0 】

上記暗号鍵処理部 3 0 には鍵レジスタ 3 4 が設けられており、また、R O M 5 0 1 には暗号鍵生成アルゴリズムおよび認証アルゴリズムをそれぞれ具現化する

プログラムが格納されていて、鍵生成&認証処理部50のCPU500は、ROM501内の暗号鍵生成アルゴリズムに従って暗号鍵を生成し、生成した暗号鍵を暗号処理回路300の鍵レジスタ34へ書き込む。また、CPU500は、認証アルゴリズムに従って認証処理を行なう。

【0031】

以下、図8を用いて上記実施例の認証通信用LSIを備えたAV機器間の認証処理および暗号処理の手順を詳細に説明する。

【0032】

記録再生装置400に蓄積または伝送されるデジタルコンテンツをAV機器800AからAV機器800Bへ送信する際には、先ず暗号化されたデジタルコンテンツを受信したいAV機器800Bから1394バスを介してAV機器800Aに対して認証を要求する通信コマンドに機器の情報を付加して送信する。認証要求コマンドを受信したAV機器800AのCPU500は、ROM501に記録されている認証処理プログラムを実行して認証処理を行い、認証処理が成功した場合はその電子機器を不正ではない電子機器であると認知する。

【0033】

認証が成立すると、AV機器800Aの鍵生成&認証処理部50において、デジタルコンテンツの暗号鍵K_{cont}を、AV機器800Bで生成するために必要な情報である乱数値seedおよび認証鍵K_{auth}を用いて交換鍵K_xに変換する暗号化処理を行なって暗号交換鍵K_{sx}を生成して、CPUバス41-1394リンク回路1001394-PHYチップ700-1394バス810を介してAV機器800Bへ送信する。

【0034】

一方、AV機器800Bでは1394バス810からの通信コマンドを、1394PHYチップ700、1394リンク回路100およびCPUバス41を経由して鍵生成&認証装置50に渡し、受信した乱数値seedおよび暗号交換鍵K_{sx}を、自己が保有している認証鍵K_{auth}を用いて復号する復号処理を行ない、復号された交換鍵K_xを用いてAV機器800A側の暗号鍵K_{cont}と同一の暗号鍵K_{cont}を得ることで、自電子機器と相手電子機器で交換鍵K_xを共有する。

【 0 0 3 5 】

続いて、AV機器800Aは、ROM501に記録されている鍵生成処理プログラムを実行して、交換鍵K_xおよび乱数値seedから暗号鍵K_{cont}を生成し、暗号処理回路300の鍵レジスタ34へ設定する。すると、暗号処理回路300は、自機器の外部デバイス90から入力される例えばMPEG2-TSパケットに乗せられた平文データからなるデジタルコンテンツを、上記暗号鍵K_{cont}を用いて暗号化し、暗号文データとして出力し、パケット処理回路101に設けられているバッファ（図示省略）に蓄え、IEEE1394で規定されるパケットの構築を行う。このとき、前記バッファは1394バス810への転送が1394リンク回路100で可能となるまで保持することで、上位層バス22の伝送速度と下位層バス12の伝送速度の相違を吸収する緩衝メモリの役割を果たす。

【 0 0 3 6 】

そして、1394リンク回路100が1394バス810へのデータ転送が可能となった時点で下位層バス12から1394PHYチップ700へ前記デジタルコンテンツが暗号化された1394パケットデータを出力し、1394PHYチップ700は1394バス810を経由して、相手AV機器へデジタルコンテンツの伝送を開始する。さらに、AV機器800Aは、相手AV機器800Bで復号するための情報として乱数値seedを、1394バス810を経由してAV機器800Bへ送信する。AV機器800Bでは、認証鍵K_{auth}を用いて暗号交換鍵K_{sx}を復号した交換鍵K_xおよび受信した前記乱数値seedを用いて、自機器の鍵生成&認証処理部50で自機器のROM501内の鍵生成処理アルゴリズムに従って、受信した暗号化デジタルコンテンツを暗号処理回路300で復号化させる処理を行う。そして、復号されたデジタルコンテンツは、外部デバイス90を介してAV機器800Bの記録再生装置400へ記録または再生される。

【 0 0 3 7 】

上記第1実施形態の認証通信用LSIにおいては、一連の処理の間、認証処理過程および鍵生成処理過程で発生するROM501のプログラムアクセスに伴なうデータおよびCPU作業中にRAM502へ格納される一時データが、CPU

バス 4 1 上に乗ることになるが、従来は別チップで構成されていた認証処理装置と暗号処理装置とが一つの半導体チップ上に形成されているため、暗号処理装置の外部端子を直接観測する場合に比べて外部からのバスの観測のみでチップ内の処理過程の細部を解析することが困難になる。

【 0 0 3 8 】

また、実施例の認証通信用 L S I は、鍵レジスタ 3 4 への設定が、唯一 C P U 5 0 0 から行えるように C P U バス 4 1 が制御されるように構成することができる。そのため、外部から C P U バス 4 1 への入力で鍵レジスタ 3 4 を設定することができないので、認証通信用 L S I を搭載した機器の改造が困難になる。さらに、1 チップ化されたことにより、コストダウンが図れるとともに、機器の部品点数を減らし、実装密度を高めることができる。

【 0 0 3 9 】

図 2 は、本発明の第 2 の実施形態を示す。この第 2 の実施形態は第 1 の実施形態とほぼ同様な構成を備えており、異なる点は、①下位層インターフェース部 1 0 に異種の packets 処理例えば M P E G 2 - T S の packets 構築を行う第 1 の packets 処理回路 1 0 1 と、I E C 6 1 8 8 3 のような暗号化が不要なデジタルコンテンツの packets 構築を行う第 2 の packets 処理回路 1 0 2 と、A N S I (Ame-rican National Standard Institute) N C I T S 325-1998 で規格が進められている S B P - 2 (Serial Bus Protocol 2) のようなデジタルデータの packets 構築を行う第 3 の packets 処理回路 1 0 3 とを備え、暗号化が不要なデジタルコンテンツは伝送線 2 1 1, 2 1 2 を介して直接 packets 処理回路 1 0 2 または 1 0 3 と上位層インターフェース部 2 0 との間で伝送されるように構成されている点と、②上位層インターフェース部 2 0 が、暗号処理回路 3 0 0 からの packets または第 2 の packets 処理回路 1 0 2 からの packets を選択して上位層バス 2 2 1 への伝送を可能とする上位層インターフェース回路 2 0 1 と、第 2 の packets 処理回路 1 0 2 からの packets または第 3 の packets 処理回路 1 0 3 からの packets を選択して上位層バス 2 2 2 への伝送を可能とする上位層インターフェース回路 2 0 2 とで構成されている点と、③上位層インターフェース回路 2 0 1, 2 0 2 を介して複数の外部デバイス 9 0 ~ 9 3 を同時に接続できるように構成され

ている点の3つである。この実施例では、パケット処理回路102, 103と1394リンク回路100とはバス111によって接続されている。また、パケット処理回路102と上位層インターフェース回路201, 202はバス211によって接続されている。パケット処理回路103と上位インターフェース回路202はバス212によって接続されている。他の構成および各種処理の手順並びに作用効果は第1の実施形態と同様であるので、説明は省略する。

【0040】

図3は、本発明の第3の実施形態を示す。この第3の実施形態は第1の実施形態とほぼ同様な構成を備えており、異なる点は、①暗号処理部30に2つの暗号処理回路300および302を備えるとともに、下位層インターフェース部10に例えばMPEG2-TSのパケット構築を行う2つのパケット処理回路101、104を、また上位層インターフェース部20は暗号処理回路300, 302に対応して第1および第2の上位層インターフェース回路200, 203を備え、暗号化を必要とするデジタルコンテンツの転送を2系統同時に行なえるように構成されている点と、②上位層インターフェース回路200, 203を介して複数の外部デバイス91, 92を同時に接続できるように構成されている点の2つである。他の構成および各種処理の手順並びに作用効果は第1の実施形態と同様であるので、説明は省略する。

【0041】

図4は、本発明の第4の実施形態を示す。この第4の実施形態は、第1の実施形態においてチップの外部に設けられていた電氣的に書換え可能な不揮発性メモリ740を内部不揮発性メモリ503として設けたものである。

【0042】

第1～第3の実施形態の認証通信用LSIにおいては、チップの外部に設けられたメモリ740が内部バス41に接続されており、認証処理から鍵生成処理までの一連の処理の間、認証処理過程および鍵生成処理過程で発生するROM501のプログラムアクセスに伴うデータおよびCPU作業中にRAM502へ格納される一時データがCPUバス41上に乗るため外部から観測できることとなるが、図4の実施形態の認証通信用LSI70では、CPUバス41がチップの

外部端子と接続されないように構成されているため、処理過程をチップ外部から観測されることはない。また、鍵レジスタ 3 4 への設定は、唯一 CPU 5 0 0 から行えるように CPU バス 4 1 が制御されるように構成されているため、外部から CPU バス 4 1 への入力で鍵レジスタ 3 4 を設定することはできないため、改造が困難である。

【 0 0 4 3 】

図 5 は、本発明の第 5 の実施形態を示す。この第 5 の実施形態は、第 1 の実施形態においてチップの外部に設けられていた下位層デバイスである 1 3 9 4 P H Y 回路 7 0 0 を認証通信用 L S I 7 0 と同一チップ内に設けたものである。1 3 9 4 P H Y 回路 7 0 0 も含めて 1 チップ化されたことにより、さらにコストダウンが図れるとともに、機器の部品点数を減らし、より一層実装密度を高めることができる。

【 0 0 4 4 】

図 6 は、本発明の第 6 の実施形態を示す。第 6 の実施形態は、内部不揮発性メモリ 5 0 3 をチップ内部に設けた第 4 の実施形態の認証通信用 L S I 7 0 において、さらに 1 3 9 4 P H Y 回路 7 0 0 をも同一チップ内に設けたものである。この実施形態によれば、第 4 の実施形態の有する効果に加えて第 5 の実施形態の有する効果をも奏することができる。

【 0 0 4 5 】

図 9 は、本発明を適用した 5 C - D T P C 仕様の認証通信用 L S I の他の実施形態を示す。この実施形態では、図 1 の実施形態の L S I にさらにシステム全体を制御するホスト CPU 8 2 との間のシリアル通信を行なう通信回路 8 0 と、外部メモリ 7 4 0 と内部バス 4 1 との接続切換えなどの制御を行なうバス制御回路 6 0 とを設けたものである。図に示されているように、通信回路 8 0 は内部バス 4 1 とホスト CPU 8 2 との間に設けられており、シリアル通信線 8 1 を介してホスト CPU 8 2 と接続されている。また、外部メモリ 7 4 0 は外部バス 6 1 を介してバス制御回路 6 0 に接続されている。

【 0 0 4 6 】

このように、本実施例においては、内部バス 4 1 がバス制御回路 6 0 と通信回

路 8 0 とにより外部から分離されており、内部バス上の信号を直接外部端子からモニタすることができない構成とされている。これによってデータの秘匿性が向上されるとともに、クラッカーによる認証アルゴリズムや暗号鍵生成アルゴリズムの解析を一層困難にすることができる。さらに、本実施例においては、内部 CPU 5 0 0 はホスト CPU 8 2 からの所定のコマンド以外を受けつけないように構成されており、CPU 5 0 0 に不正なコマンドを与えて RAM 5 0 2 や ROM 5 0 1 のデータをチップ外部に読み出すようなことができない構成とされている。

【 0 0 4 7 】

図 1 0 は、本発明を適用した認証通信用 L S I のさらに他の実施形態を示す。この実施形態では、図 9 の実施形態の L S I におけるホスト CPU 8 2 との間のシリアル通信を行なう通信回路 8 0 を省略し、外部メモリ 7 4 0 と内部バス 4 1 との間にバスの接続切換えなどの制御を行なうバス制御回路 6 0 を設けたものである。

【 0 0 4 8 】

図 1 1 は、本発明を適用した認証通信用 L S I のさらに他の実施形態を示す。この実施形態では、図 9 の実施形態の L S I におけるホスト CPU 8 2 との間のシリアル通信を行なう通信回路 8 0 を省略し、外部メモリ 7 4 0 と内部バス 4 1 との間にバスの接続切換えなどの制御を行なうバス制御回路 6 0 を設けるとともに、上位層と下位層の外部インタフェース回路 1 0 , 2 0 のうち下位層の外部インタフェース回路 1 0 のみを設けたものである。

【 0 0 4 9 】

図 1 2 は、本発明を適用した認証通信用 L S I のさらに他の実施形態を示す。この実施形態では、図 9 の実施形態の L S I におけるホスト CPU 8 2 との間のシリアル通信を行なう通信回路 8 0 を省略し、外部メモリ 7 4 0 と内部バス 4 1 との間にバスの接続切換えなどの制御を行なうバス制御回路 6 0 を設けるとともに、上位層と下位層の外部インタフェース回路 1 0 , 2 0 のうち上位層の外部インタフェース回路 2 0 のみを設けたものである。

【 0 0 5 0 】

図 1 0 ～ 図 1 2 の実施形態においても、内部バス 4 1 がバス制御回路 6 0 によって外部バス 6 1 と切り離されているので、不正コピー防止上、図 9 の実施形態の認証通信用 L S I とほぼ同様の利点を有している。また、図 1 1 および図 1 2 の実施形態のように、暗号生成&認証処理部 5 0 と暗号処理部 3 0 と上位層と下位層の外部インタフェース回路 1 0, 2 0 のうち一方とが 1 つのチップ上に形成されていれば、暗号処理部 3 0 に入出力される平文データと暗文データを直接対比して暗号鍵を推定することができないため、データの秘匿性を高めることができる。

【 0 0 5 1 】

以上本発明者によってなされた発明を実施例に基づき具体的に説明したが、本発明は上記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば図 4 ～ 図 1 2 の実施例において、図 2 や図 3 の実施例のように、複数のパケット処理回路や複数の上位インタフェース回路を設けて、複数のパケットデータの転送を同時に行なえるように構成しても良い。以上の説明では主として本発明者によってなされた発明をその背景となった利用分野である 5 C - D T P C 仕様の認証通信用 L S I に適用下場合について説明したが、本発明は DVD-Video の C S S 仕様の通信用 L S I にも利用することができる。また、本発明を適用した認証通信用 L S I は、デジタルビデオテープレコーダや I R D (Integrated Receiver/Decoder) などの A V 機器のみならずパーソナルコンピュータなどにも利用することができる。

【 0 0 5 2 】

【発明の効果】

本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記のとおりである。すなわち、本発明に従うと、半導体チップの内部信号を外部から窃取しにくいとともに、認証処理過程の通信コマンドや暗号処理過程の暗号鍵設定を認証通信用 L S I の外部から改竄して入力することが困難であるので、不正コピー防止技術を破るために認証処理過程を解析することが困難となり、また、電子機器を改造して不正コピー防止技術を破ることが難しくなり、これによって、著作権保護を必要とするデジタルコンテンツを高い安全

性の下に送受信できる電子機器を実現することができる。

【図面の簡単な説明】

【図 1】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器の第 1 の実施形態を示すブロック図である。

【図 2】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器の第 2 の実施形態を示すブロック図である。

【図 3】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器の第 3 の実施形態を示すブロック図である。

【図 4】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器の第 4 の実施形態を示すブロック図である。

【図 5】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器の第 5 の実施形態を示すブロック図である。

【図 6】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器の第 6 の実施形態を示すブロック図である。

【図 7】

図 1 の構成を有する 2 つの A V 機器を I E E E 1 3 9 4 シリアルバスに接続した場合の説明図である。

【図 8】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器における認証処理および暗号処理の過程説明図である。

【図 9】

本発明を適用した認証通信用 L S I およびそれを搭載した A V 機器の第 7 の実施形態を示すブロック図である。

【図 1 0】

図 9 の実施形態の変形例を示すブロック図である。

【図 1 1】

図 9 の実施形態の変形例を示すブロック図である。

【図 1 2】

図 9 の実施形態の変形例を示すブロック図である。

【図 1 3】

従来の認証通信装置およびそれを搭載した A V 機器の一例を示すブロック図である。

【図 1 4】

従来の認証通信装置を用いた A V 機器における不正改造の例を示す説明図である。

【符号の説明】

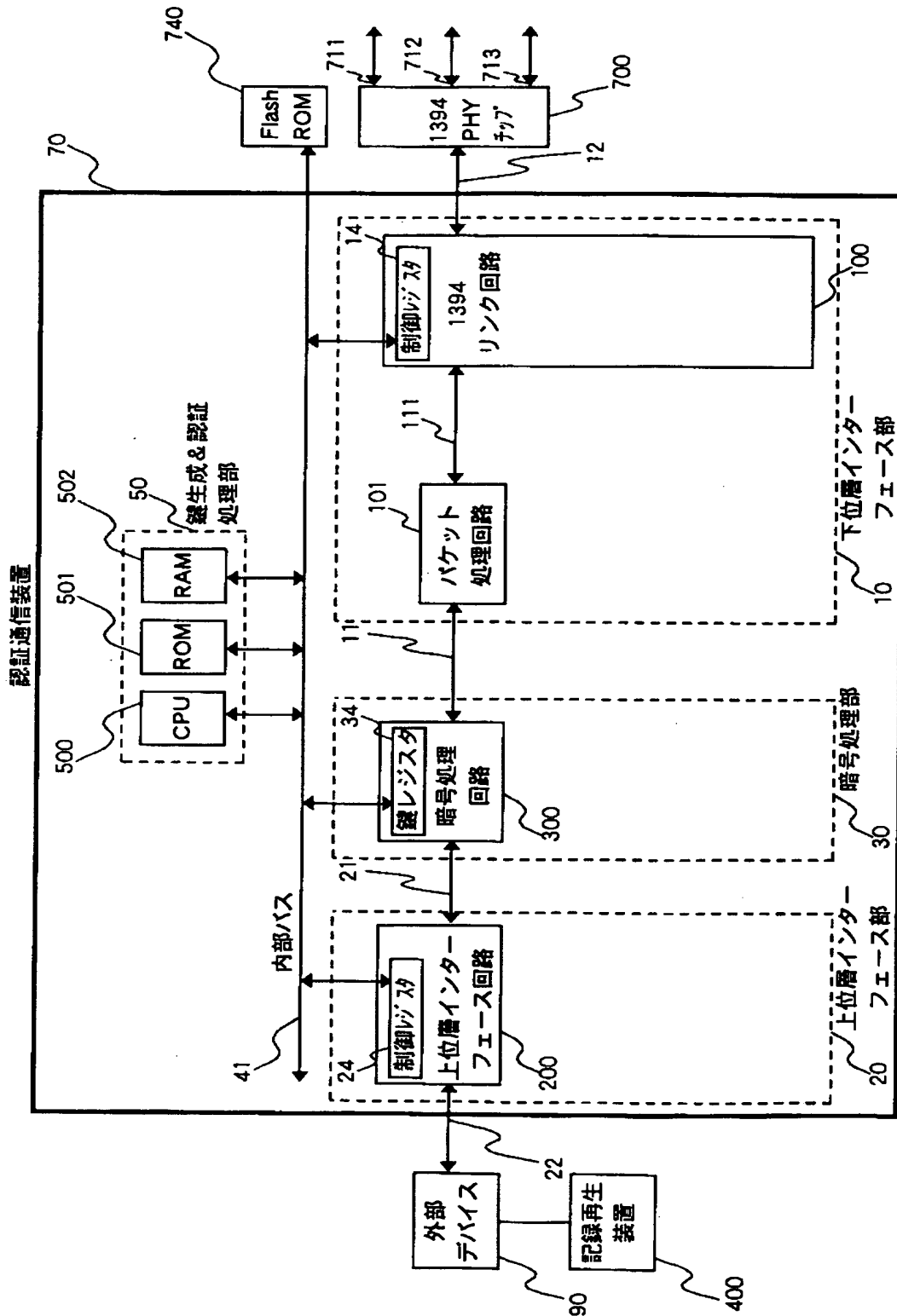
- 1 0 下位層インターフェース部
- 1 4 制御レジスタ
- 2 0 上位層インターフェース部
- 2 4 制御レジスタ
- 3 0 暗号処理部
- 3 4 鍵レジスタ
- 4 1 内部バス
- 5 0 鍵生成&認証処理部
- 7 0 認証通信装置
- 9 0 ～ 9 3 外部デバイス
- 1 0 0 1 3 9 4 規格のリンク回路
- 1 0 1 ～ 1 0 4 パケット処理回路
- 2 0 0 ～ 2 0 3 上位層インターフェース回路
- 3 0 0, 3 0 2 暗号処理回路
- 4 0 0 記録再生装置
- 5 0 0 C P U

5 0 1 ROM
5 0 2 RAM
7 0 0 1 3 9 4 PHYチップ
7 1 1 ~ 7 1 3 1 3 9 4 PHYポート
7 2 1 ~ 7 2 2 1 3 9 4 ソケット
7 3 1 ~ 7 3 3, 7 5 1 ~ 7 5 3 1 3 9 4 プラグ
7 4 1, 7 4 2 1 3 9 4 ケーブル
7 2 0 IEEE 1 3 9 4 規格のコネクタ部
7 3 0 IEEE 1 3 9 4 規格のケーブル
7 4 0 外部メモリ (フラッシュROM)
8 0 0, 8 0 0 A, 8 0 0 B AV機器
8 1 0 IEEE 1 3 9 4 規格のバス

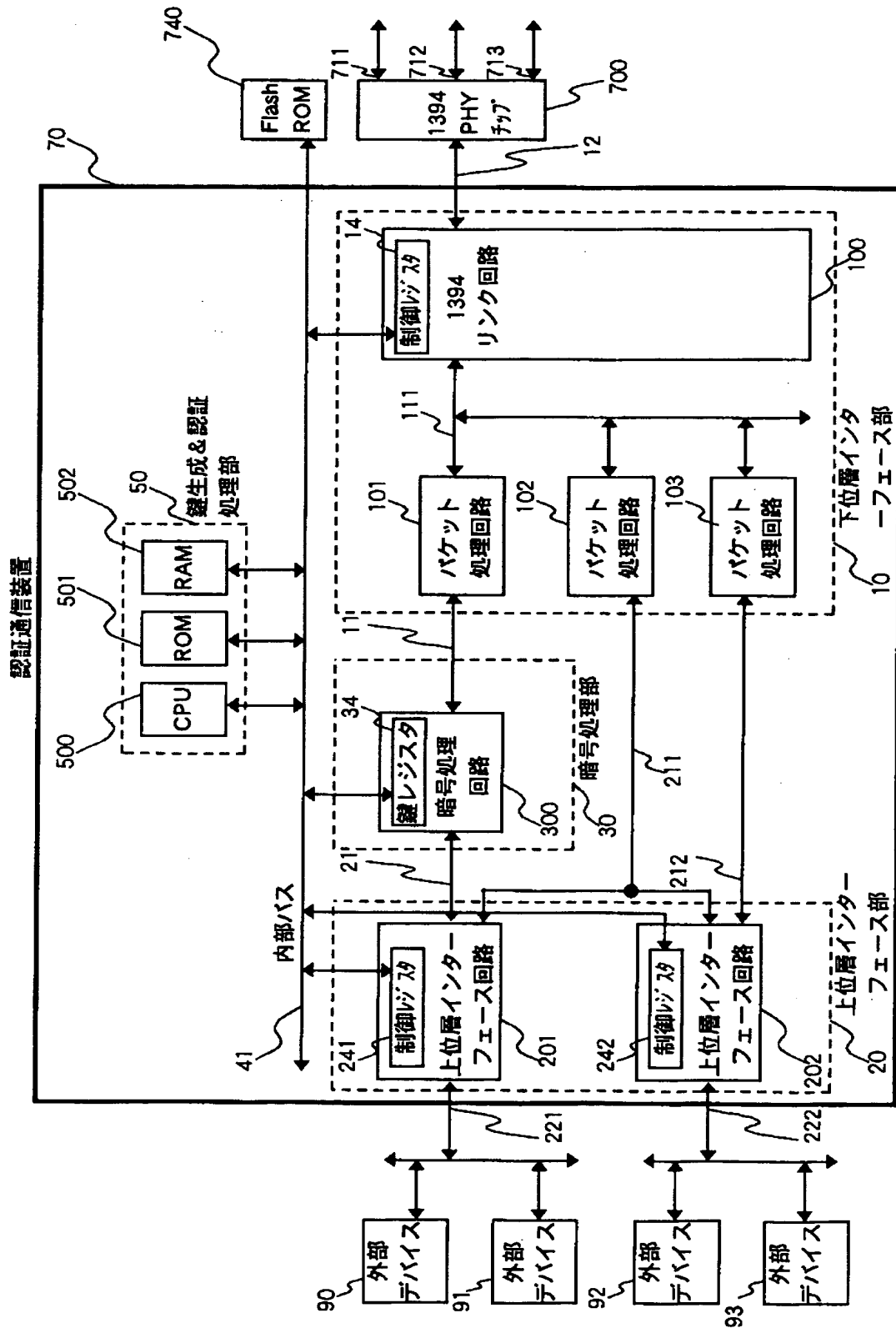
【書類名】

図面

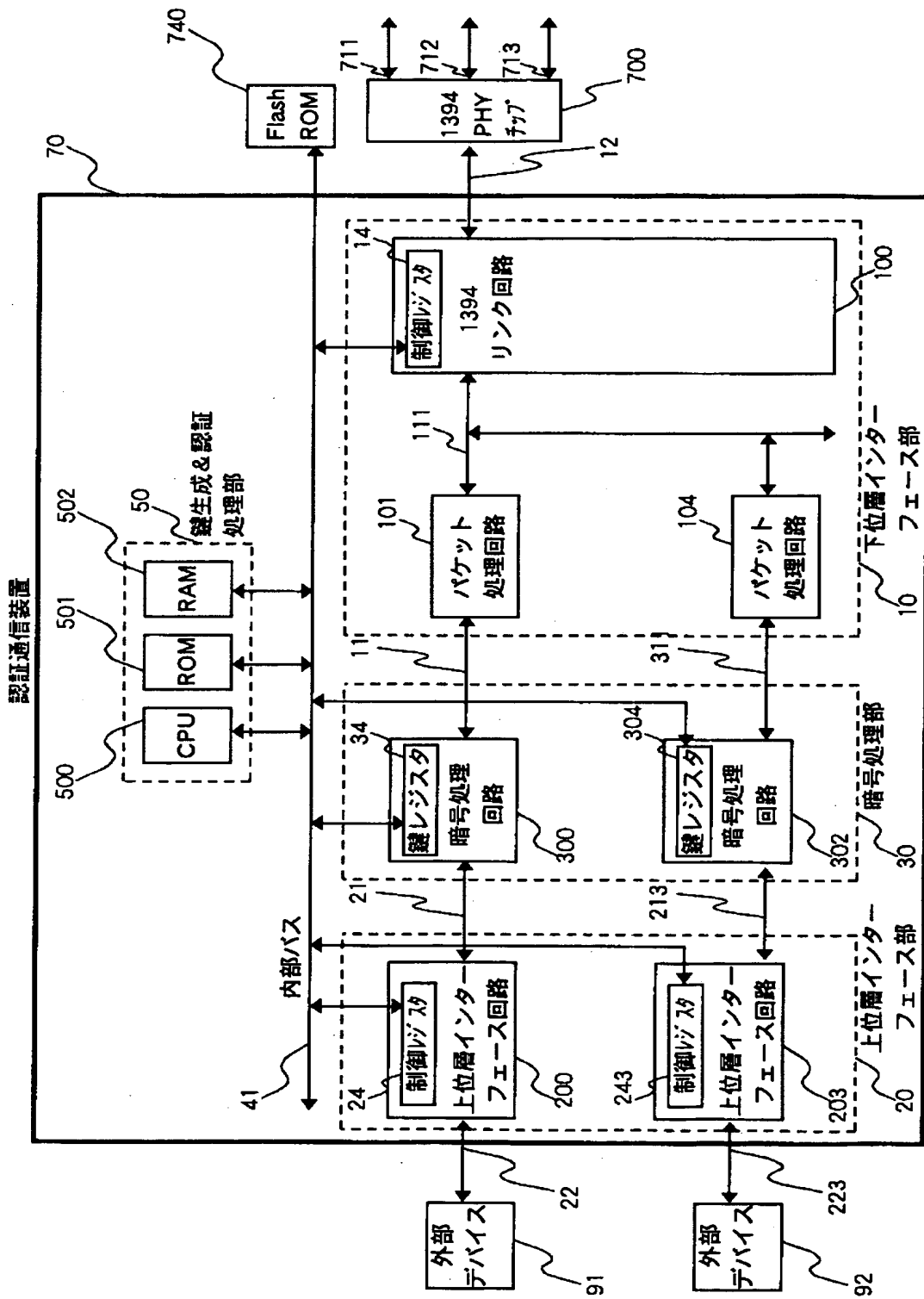
【図 1】



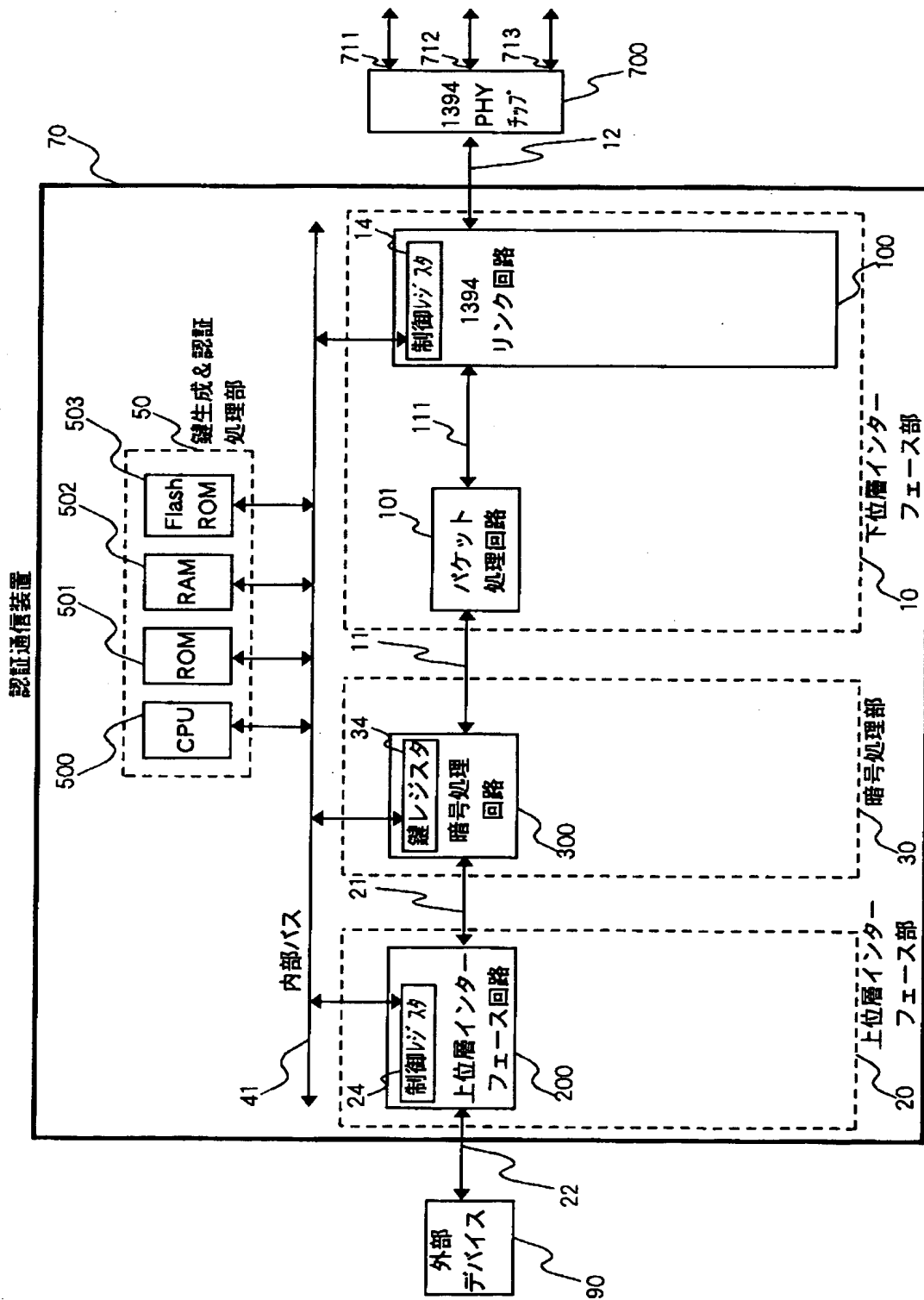
【図2】



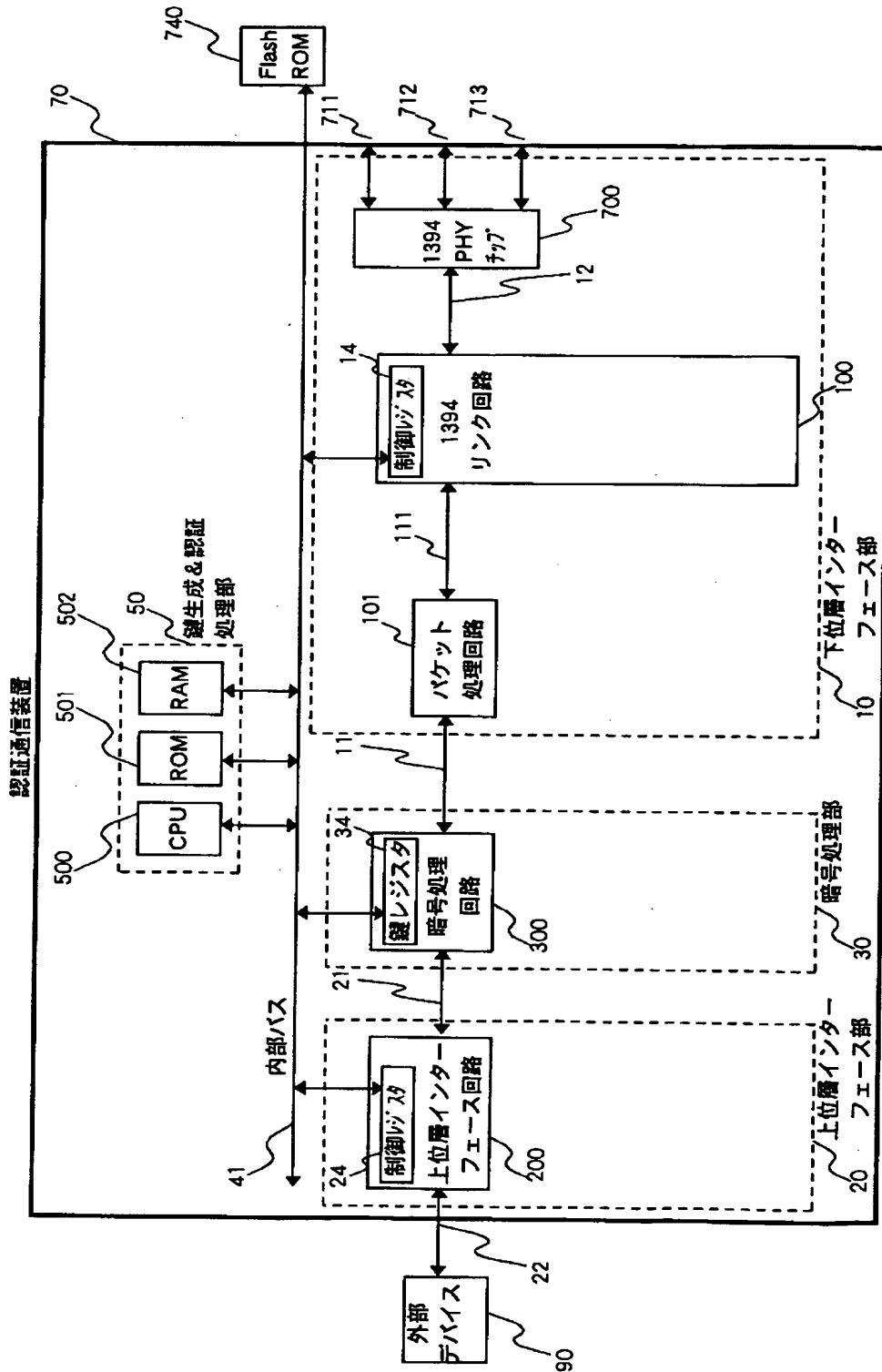
【図3】



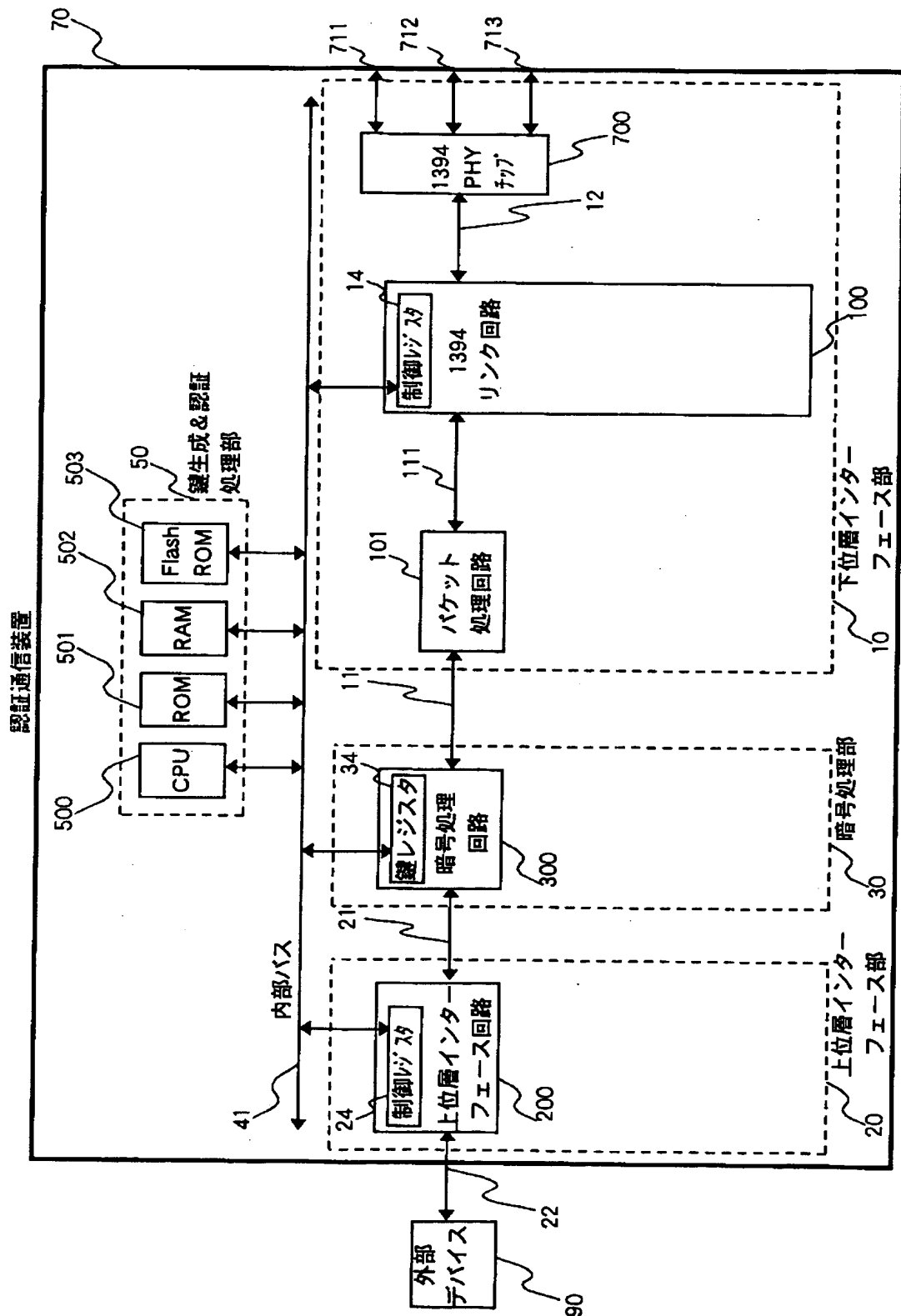
【図4】



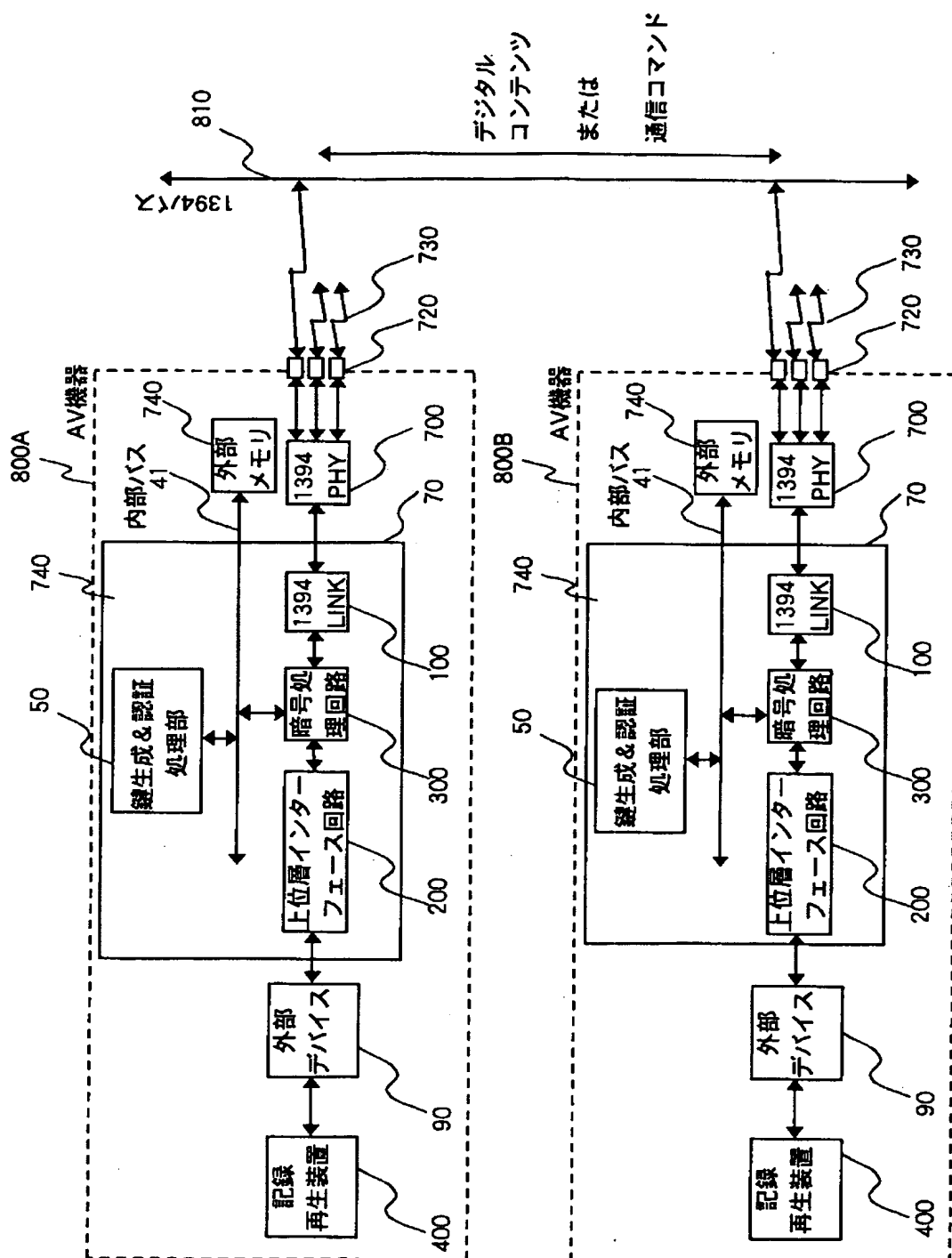
【図5】



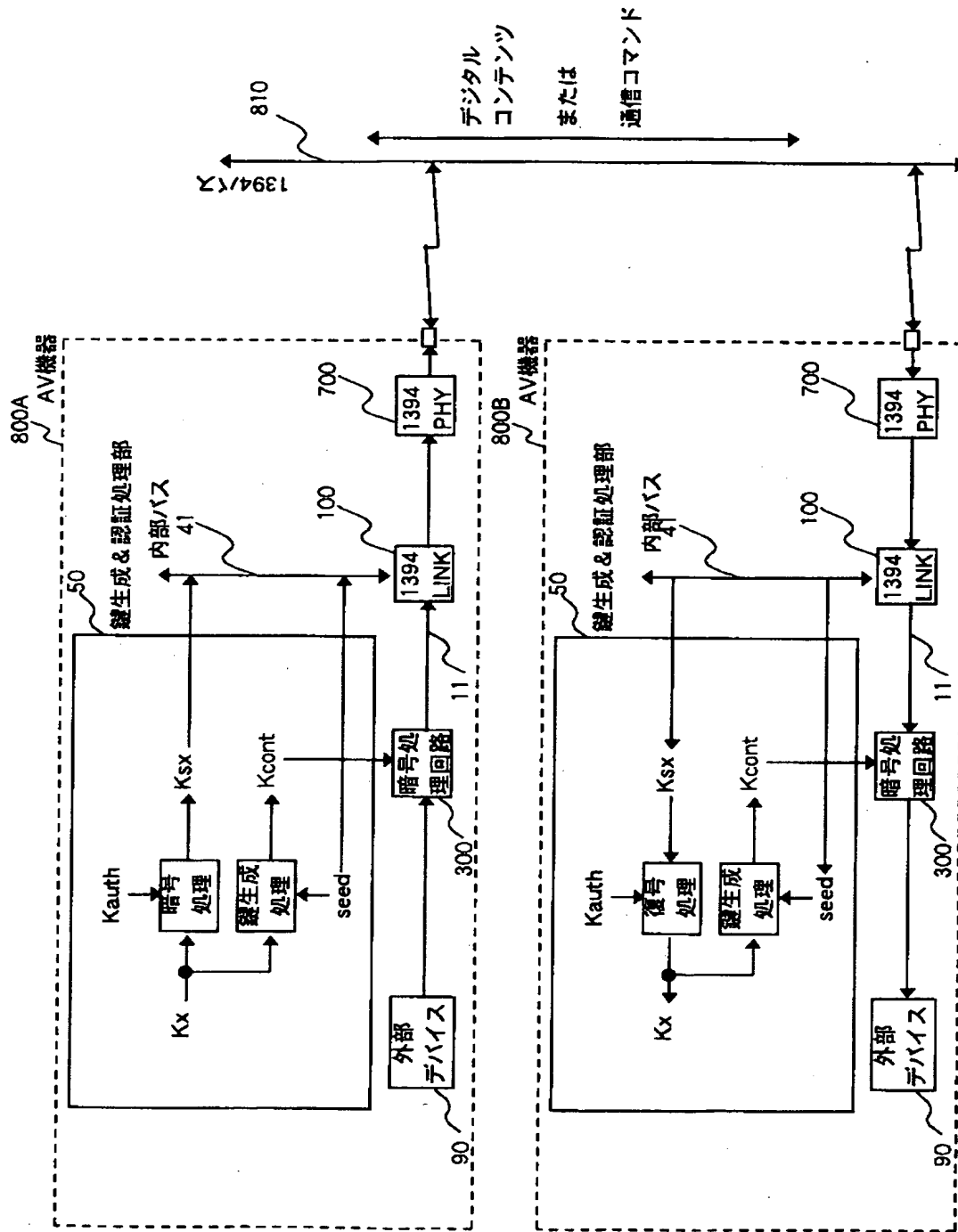
【図6】



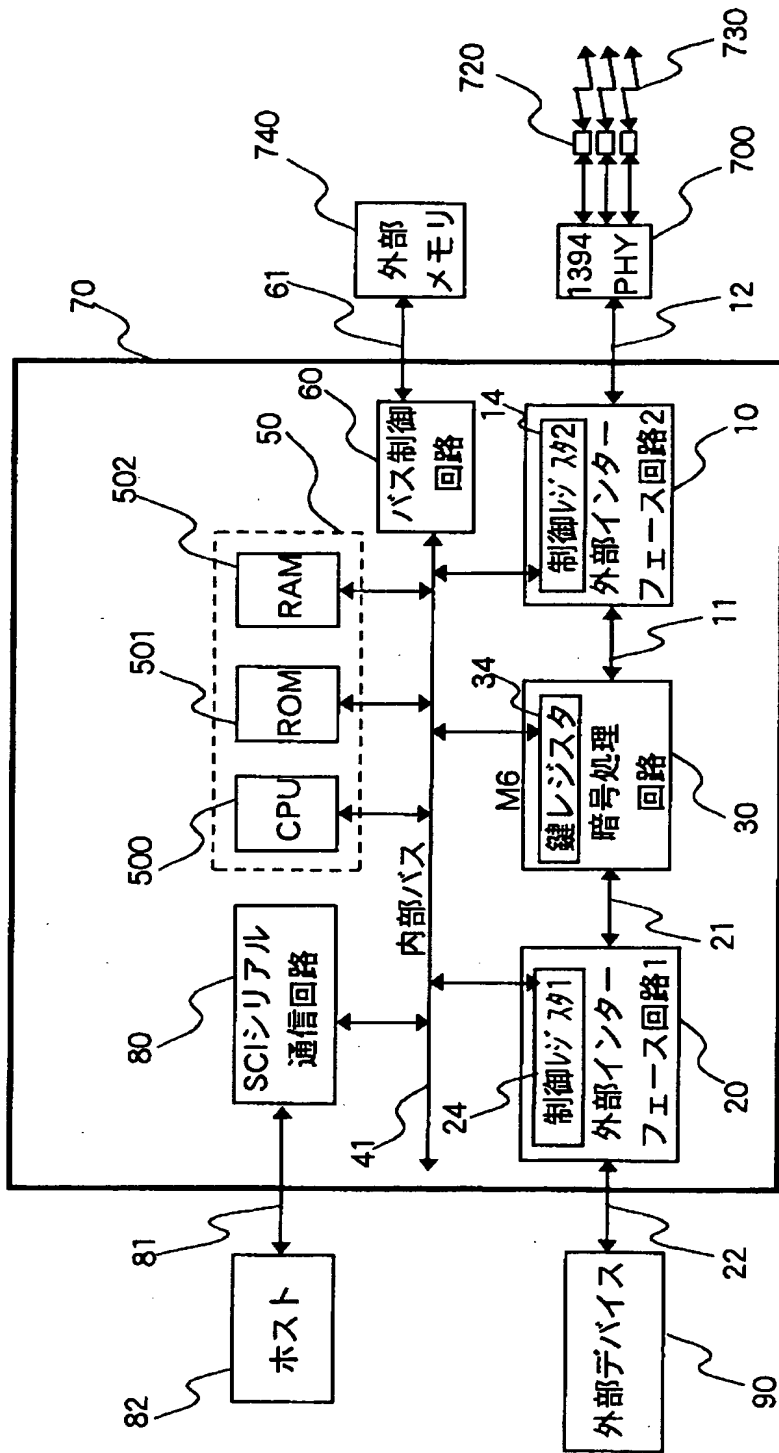
【圖 7】



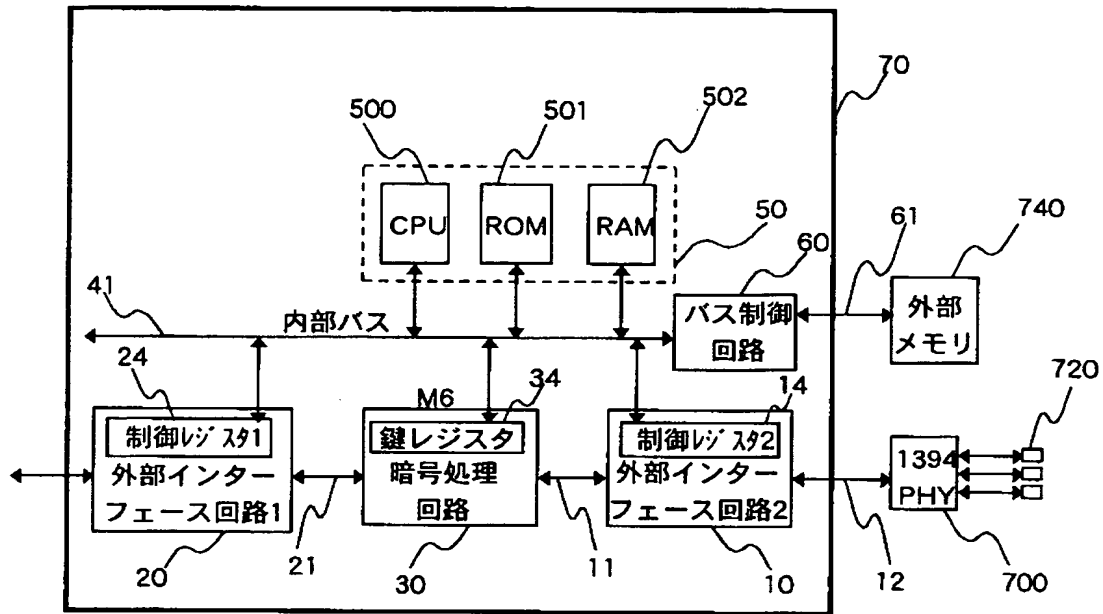
【図 8】



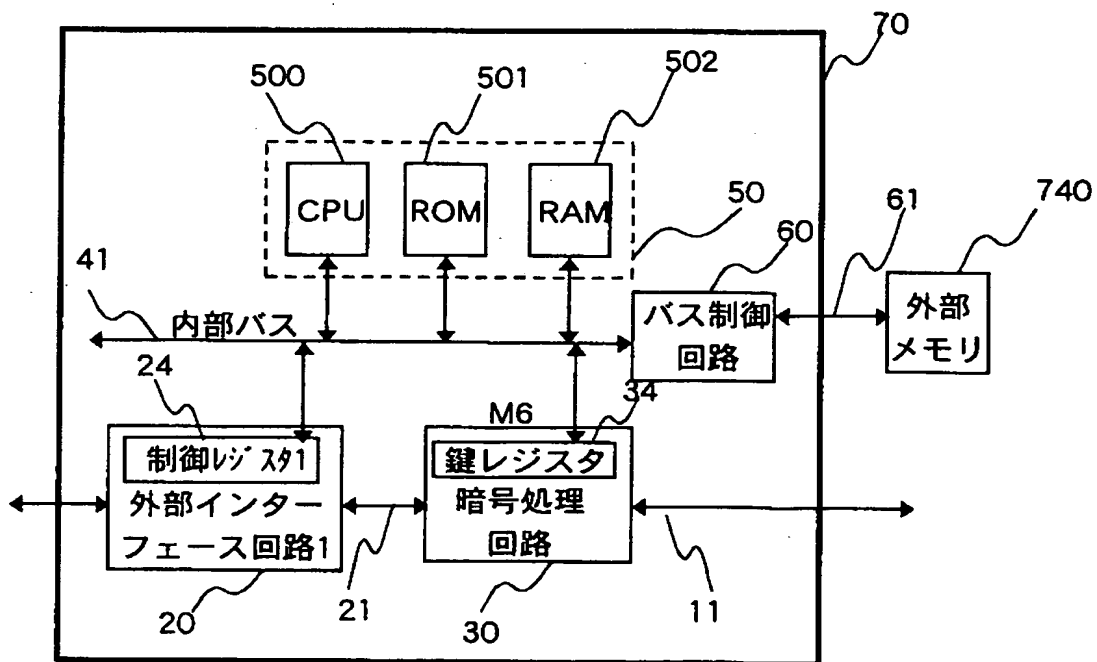
【図9】



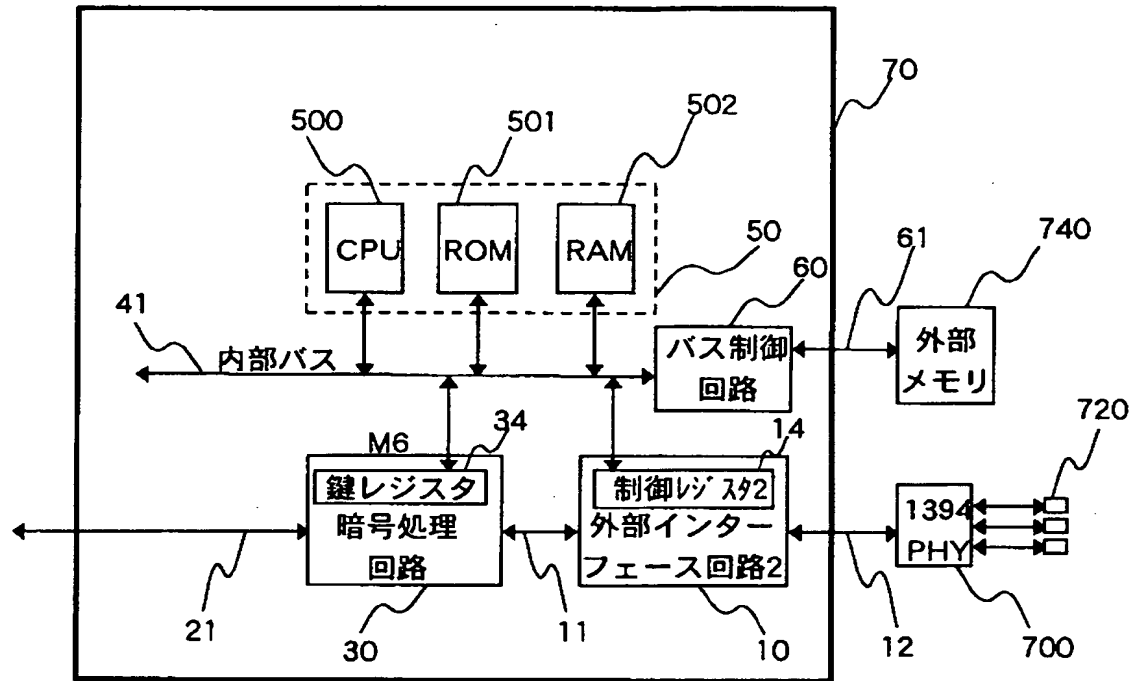
【図10】



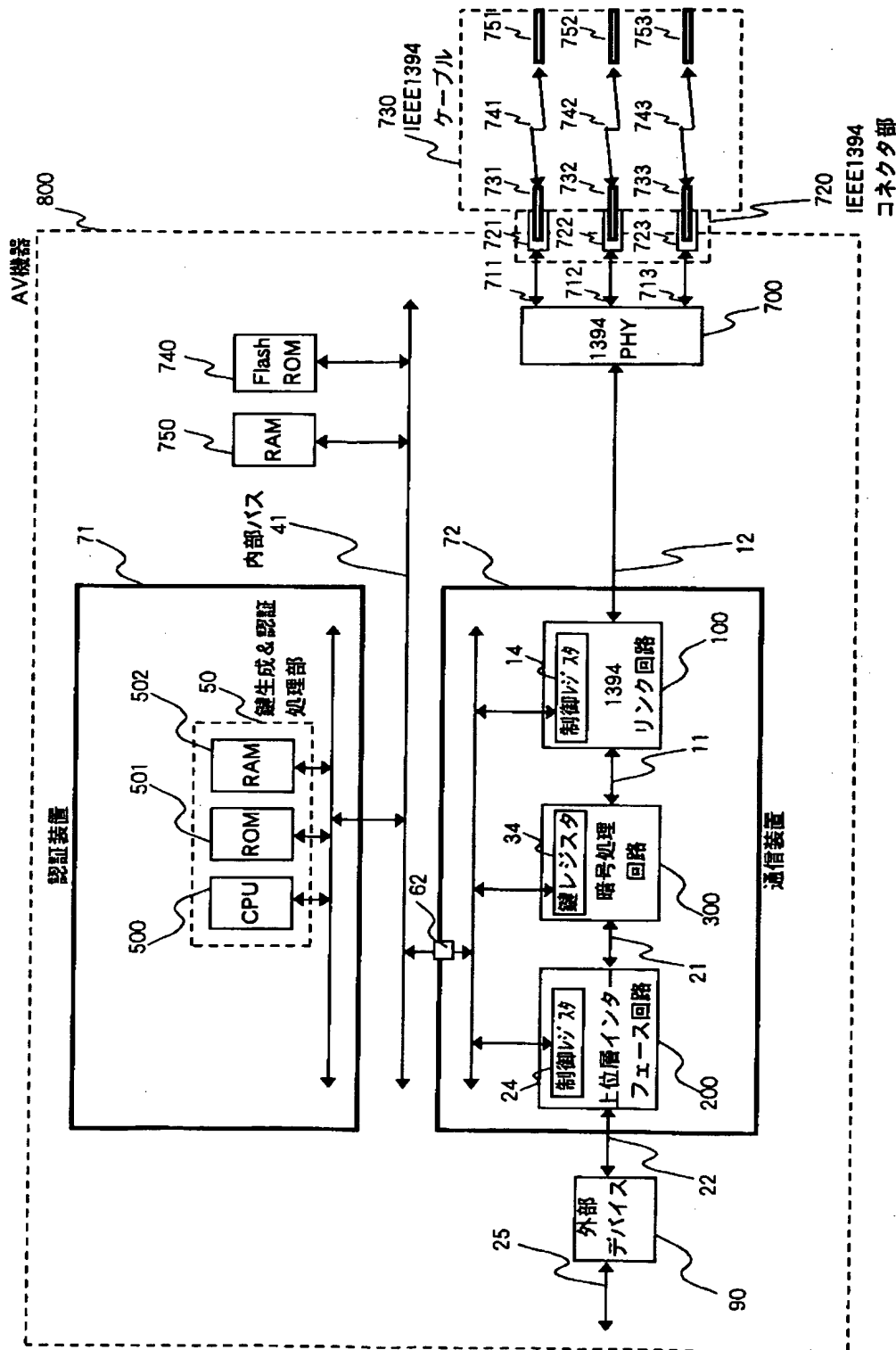
【図11】



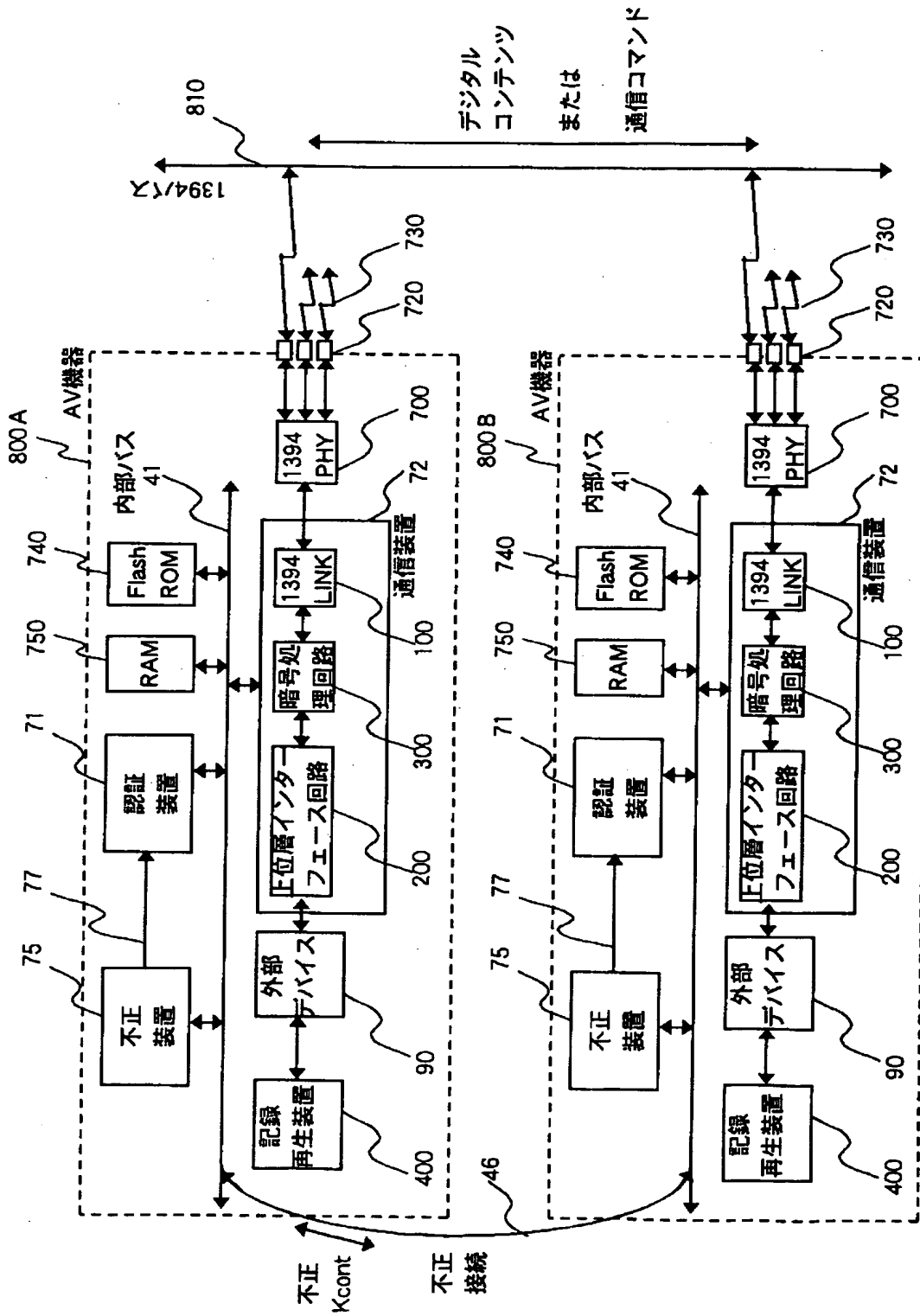
【図 1 2】



【図13】



【図 14】



【書類名】 要約書

【要約】

【課題】 不正コピー防止の技術を破るため、CPUバスにロジック・アナライザのプローブを接続するなどして、認証処理過程を窃取し解析することで不正コピー防止の仕掛けを破られる可能性があった。また、CPUバスへ改竄された暗号鍵などを設定できるような電子機器の改造のおそれがあった。

【解決手段】 1個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するとともに外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および復合化を行なう暗号処理部と、所定のプロトコルに従って上位層または下位層との通信を行なうインタフェース部とを形成して、暗号処理過程や認証処理過程での暗号鍵を装置の外部から窃取できにくくした。

【選択図】 図1

認 定 ・ 付 加 情 報

特許出願の番号	特願 2 0 0 0 - 1 5 8 7 7 0
受付番号	5 0 0 0 0 6 6 2 0 9 6
書類名	特許願
担当官	第一担当上席 0 0 9 0
作成日	平成 1 2 年 6 月 1 4 日

< 認定情報・付加情報 >

【提出日】 平成12年 5月29日

出 願 人 履 歴 情 報

識別番号 { 0 0 0 0 0 5 1 0 8 }

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

 [変更理由] 新規登録

 住 所 東京都千代田区神田駿河台4丁目6番地

 氏 名 株式会社日立製作所